

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **63-061393**

(43) Date of publication of application : 17.03.1988

(51)Int.Cl.

G06K 19/00

B42D 15/02

G11B 7/24

(21)Application number : 61-204751

(71)Applicant : DAIICHI DENSHI KOGYO KK

(22)Date of filing : 30.08.1986

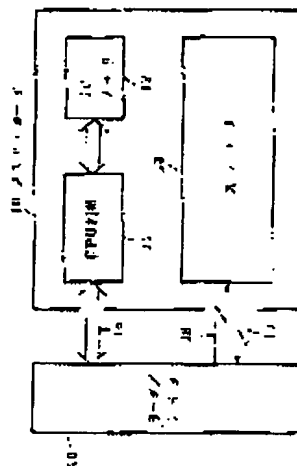
(72)Inventor : INOUE TAKAMASA

(54) MEMORY CARD

(57)Abstract:

PURPOSE: To improve a security function by accommodating the information enciphered to an optical memory.

CONSTITUTION: A memory card 10 includes a CPU circuit 11, which is a processor including a microprocessor, an IC memory 12, and a non-erasing or rewritable optical memory 13. When a cipher key K1 is transferred from a reader/writer 20 to the CPU circuit 11, the CPU circuit 11 generates a cipher key K2 and accommodates this to the IC memory 12. Thus, the CPU circuit 11 completes the preparation of a cipher processing and informs the reader/ writer 20 of it. The reader/writer 20 executes the writing or reading of the optical memory 13 and transfers the data to the CPU circuit 11. The CPU 11 receiving the data decodes the data based on the ciphering key K2 stored temporarily in the IC memory 12, enciphers them and transfers them to the reader/writer 20. The reader/writer 20 outputs the data or writes them into the optical memory 13.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑪ 公開特許公報(A)

昭63-61393

⑫ Int. Cl.

識別記号

庁内整理番号

⑬ 公開 昭和63年(1988)3月17日

G 06 K 19/00

B 42 D 15/02

G 06 K 19/00

G 11 B 7/24

3 3 1

R-6711-5B

J-8302-2C

F-6711-5B

B-8421-5D

審査請求 未請求 発明の数 1 (全4頁)

⑭ 発明の名称 メモリ・カード

⑮ 特 願 昭61-204751

⑯ 出 願 昭61(1986)8月30日

⑰ 発 明 者 井 上 専 勝 東京都渋谷区代々木2丁目7番12号 第一電子工業株式会社内

⑱ 出 願 人 第一電子工業株式会社 東京都渋谷区代々木2丁目7番12号

⑲ 代 理 人 弁理士 内田 公三

明 細 書

1. 発明の名称

メモリ・カード

2. 特許請求の範囲

(1) 記憶内容を読み出し情報を書き込むためのリーダ/ライタに用いるメモリ・カードであって、

前記リーダ/ライタと電気的に接続されて暗号処理をするための処理手段と、

前記処理手段からの指示にもとづき、すくなくとも前記暗号処理のための情報を書き込まれ読み出されるためのICメモリと、

前記リーダ/ライタによって、すくなくとも記憶内容を光学的に読み出されるための光メモリを含むことを特徴とするメモリ・カード。

(2) 前記光メモリが、前記リーダ/ライタによって書き込みも行われ得るものである特許請求の範囲第1項記載のメモリ・カード。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は半導体ICと光メモリとを内蔵するメモリ・カードに関する。とくに、記憶容量の大きな機密性に富んだ改良されたメモリ・カードを提供せんとするものである。

〔従来の技術〕

マイクロプロセッサなどを含むCPUやメモリである半導体ICを内蔵した、いわゆるICカードが使用されている。

一方ビデオ・ディスクやコンパクト・ディスクなどの光によるメモリの他、このような非消去型の光メモリをカード化したものがある。

〔発明が解決しようとする問題点〕

半導体ICによるICメモリは、集積技術の飛躍的進歩によってその記憶容量を著しく増大しているが、いまだ十分ではなく、光カードに比較してビット当たりのコストは非常に高価となっている。

また、静電気に対して極めて弱いという問題点

を有している。

これに対して、ＩＣメモリのように簡単に書き換えすることのできる光メモリは、光カードとしては製品化されてはいないが、極めて大容量で、ビット当たりのコストは安価で、記憶内容の破壊に対しては極めて強いという特徴を有している。また、最近では書き換え可能な光メモリも出現している。しかしながら、光カードは演算機能を有していないために、さらに、メモリ・パターンが可視性であるために、個人に関する情報などを記憶せしめておくには、セキュリティ面で不安があった。

このような問題があるために、光カードに情報を入出力する際には、暗号化処理をすることが必要であるが、現在の光カード自体には演算能力がないために、このような光カードのデータを読み出し、書き込みするリーダ／ライタを含む端末装置で暗号化処理を行っているが、セキュリティ機能は充分ではない。

なぜならば、端末装置において暗号化処理が行

したがって、本発明によるカードをセキュリティ・カードとして使用するならば、従来のＩＣカードによっては実現できなかった高度のセキュリティ機能を光カードによって保有することが可能となった。

〔実施例〕

本発明の一実施例を示す第１図を用いて説明する。

１０はメモリ・カードであり、そこには、マイクロプロセッサを含む処理装置であるＣＰＵ回路１１およびＩＣメモリ１２と、非消去型あるいは書き換え可能な光メモリ１３とを含んでいる。

２０は、このメモリ・カード１０を挿入されて、その記憶内容を読み出し、書き込むためのリーダ／ライタである。

これらの動作の流れの一例を第２Ａ図および第２Ｂ図に示したフローチャートにより説明する。

メモリ・カード１０の所有者が、これをリーダ／ライタ２０に挿入すると、それが本人であるか否かを確認する（Ｓ５１）。本人でない場合には

特開昭 63-61393 (2)

われているので、端末装置の暗号化処理が解読された場合には、その端末装置を利用するすべての光カードのセキュリティ機能に問題が発生するという重大な問題点があった。

〔問題点を解決するための手段〕

本発明はこのような問題点を解決するためになされたものであり、セキュリティ機能を補償するために端末装置側に暗号キーＫ１をもたせ、これを受けたカード側では暗号キーＫ２を発生し、これを書き込んだり書き換えを要する情報を記憶するためのメモリや情報処理などに一時的に要するメモリとしてのＩＣメモリと、このＩＣメモリへの書き込み読出しと、外部装置であるリーダ／ライタを介して光メモリの記憶情報を書き込み読み出し、処理するためのマイクロプロセッサを含むＣＰＵ回路とをカード内に設けた。

〔作用〕

端末装置側の暗号キーＫ１がかりに解読されたとしても、この暗号キーＫ１を受けてカード側で発生する暗号キーＫ２を解読することはできない。

本人であると確認できるまでこの確認作業は繰り返される（Ｓ５１ＮＯ）。本人であると確認すると（Ｓ５１ＹＥＳ）、ＣＰＵ回路１１（ＣＰＵ）からバス１５を介してリーダ／ライタ２０（Ｒ／Ｗ）に対してアクセス許可の指示がなされる（Ｓ５２）。

アクセス許可を受けたリーダ／ライタ２０は内蔵している暗号キーＫ１をＣＰＵ回路１１に転送する（Ｓ５３）。暗号キーＫ１を受けたＣＰＵ回路１１は、ＩＣメモリ１２から暗号キーＫ１を受けた場合の処理に関するデータを読み出して暗号キーＫ２を発生し、これをＩＣメモリに格納する（Ｓ５４）。これによってＣＰＵ回路は暗号処理の準備を完了し、それをリーダ／ライタ２０に通知する（Ｓ５５）。

そこでリーダ／ライタ２０は光メモリ１３に記憶されているデータを読み出すのか、あるいは光メモリ１３にデータを書き込むのか作業の処理内容を判断して決定する（Ｓ５６）。

読み出しに決定した場合は（Ｓ５６読出）、リ

BEST AVAILABLE COPY

特開昭63-61393 (3)

ーダ／ライタ20は、レーザ光18を光メモリ13に照射し、その反射光19を得て、データを読み出し、それをCPU回路11へ転送する(S57)。このデータを受けたCPU回路11は、ICメモリ12に一時的に記憶してある暗号キーK2にもとづき解読し、解読データをリーダー／ライタ20へ転送する(S61)。

この解読されたデータを受けたリーダー／ライタ20では、これを処理して、表示したり、あるいは必要に応じてプリントなどして(S62)、その結果、光メモリ13に書き込むべきものがあるか否かを判断し(S63)、書き込むべきものがない場合には(S63NO)、ICメモリ12に書き込むべきものがあるか否かを判断し(S64)、ICメモリ12に書き込みを要する場合には(S64YES)、書き込んだ(S65)後に、また、書き込み不要の場合には(S64NO)、そこで作業を終了する。

ステップS56で光メモリ13に書き込みを要するとされた場合(S56肯定)、およびS63

で光メモリ13に書き込みを要するとされた場合(S63YES)には、リーダー／ライタ20から書き込み情報をCPU11へ転送し(S66)、CPU11ではICメモリ12に記憶してある暗号キーK2にもとづいて暗号化し、その暗号化したデータをリーダー／ライタ20へ転送し(S67)、リーダー／ライタ20は、図示されてはいない強いレーザ光によって、光メモリ13に書き込み作業をして終了する(S68)。

以上の説明は、光メモリ13が読み出し書き込み可能な場合について例示的に説明したが、光メモリ13が読み出し専用である場合には、S56、S63、S66、S67、S68の各ステップが省略される。

以上の説明においては、読み出し、書き込みには、レーザ光を用いた場合を例示したが、それ以外の光、たとえば読み出しにおいては、しばしば用いられるハロゲン・ランプの光を用いることも可能である。

〔発明の効果〕

以上の説明から明らかなように、本発明によるならば、安価で大容量を有する光メモリに、暗号化した情報を格納しておくことができるから、セキュリティ機能が著しく向上し、従来のICカードや光カード単体では果せなかった機能を、安価に実現することができる。これにより、たとえば、本人を確実に確認することができ、その後に受けるサービス用の情報は、ICメモリや光メモリに適宜に記憶せしめるように用いることができるから、本カードは極めて便宜に使用されるものである。

さらに、メモリ・カード単位でセキュリティ機能が保証されるから、端末装置内部に保存されている暗号キーや暗号処理アルゴリズムの保守や管理、さらには端末装置管理者の監督などは、ほとんど不要となり、1枚のメモリ・カードの暗号キーが、かりに解読されても、他のメモリ・カードには影響が出ないという特色を有している。個々のメモリ・カードの暗号処理アルゴリズムはメモリ・カードごとに各種のものを選択し適用するこ

とが可能であるから、セキュリティ機能は格段に勝れたものが得られる。したがって本発明の効果は極めて大きい。

4. 図面の簡単な説明

第1図は本発明の一実施例を説明するための回路構成図、

第2A図および第2B図は、第1図に示したものの動作例を示すためのフローチャートである。

10…メモリ・カード
11…CPU回路 12…ICメモリ
13…光メモリ 15…バス
18…レーザ光 19…反射光
20…リーダー／ライタ。

代理人 内 田 公 三

BEST AVAILABLE COPY

特開昭 63-61393 (4)

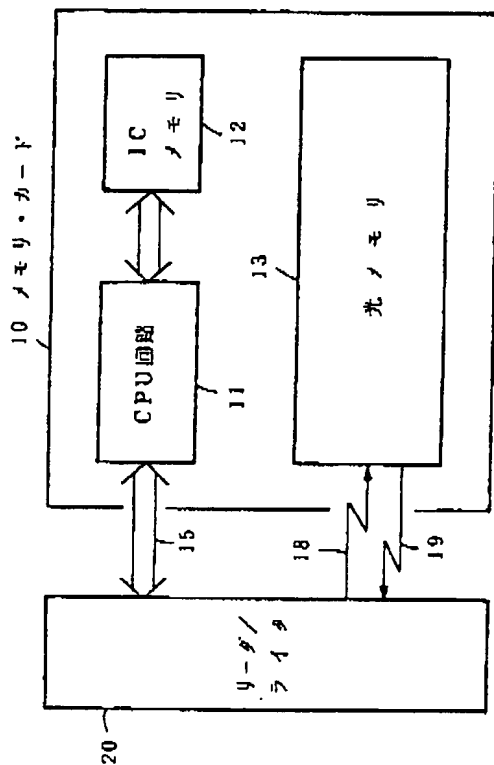
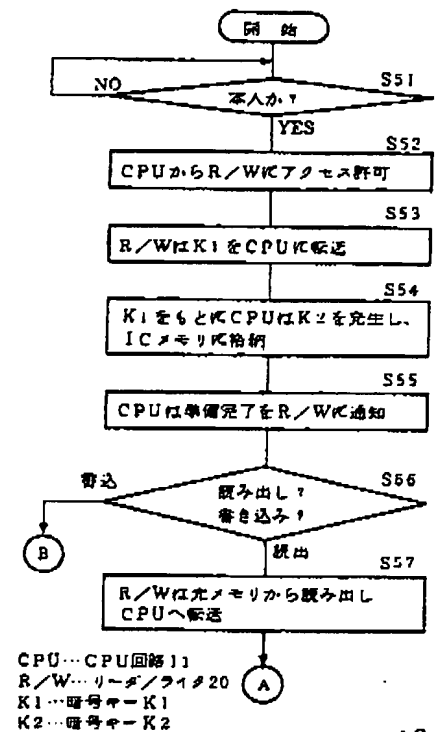
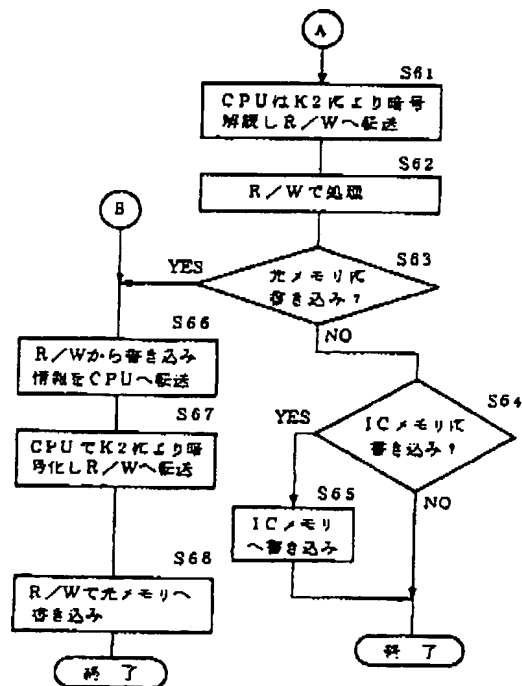


図 1



第2A図



第2B図